

## § 95.31

through the use of a cleared employee or by a CSA approved access control device or system.

(2) Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matter within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

(3) The Closed Area must be accorded supplemental protection during non-working hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.

(4) Open shelf or bin storage of classified matter in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

[62 FR 17693, Apr. 11, 1997, as amended at 64 FR 15652, Apr. 1, 1999]

## § 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information they shall:

(a) Possess an "L" access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a "Q" access authorization (or CSA equivalent) if the licensee, certificate holder, or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval Nuclear Propulsion Program information (e.g., fuel manufacturing technology) and the protective

## 10 CFR Ch. I (1–1–10 Edition)

personnel require access as part of their regular duties.

[72 FR 49562, Aug. 28, 2007]

## § 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

(a) *Facility Security Officer training.* Licensees and others are responsible for ensuring that the Facility Security Officer, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer.

(b) *Government-provided briefings.* The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) *Temporary help suppliers.* A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee's, certificate holder's, or other person's facility may conduct these briefings.

(d) *Classified Information Nondisclosure Agreement (SF-312).* The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of § 25.23 of this chapter, execute an SF-312 before being granted access to classified information. The Facility Security Officer shall forward